KCELL SECURITY POLICY

Kcell JSC (hereinafter referred to as the "Kcell") has adopted the principles stated in this Policy which is based on the Telia Company Group Security Policy.

BACKGROUND AND DESCRIPTION

Background

This Policy relates to Security and is a binding for Kcell and its Subsidiaries.

Terms starting with a capital letter in this Policy are defined in the Delegation of Obligations and Authority.

Description

This is the Kcell Security Policy stating the mandatory security requirements for the Kcell.

Security is an integral part of sound governance. The governance of security within Kcell is coordinated by Security Section in cooperation with all parts of the organization. It aims to control, facilitate and implement well-balanced security measures throughout our operation.

SCOPE AND PURPOSE

Scope

This Policy applies to Kcell and for its Subsidiaries. For subsidiaries, this Policy implies as their own binding policy.

This Policy is part of the Group Governance Framework, which includes without limitation:

a) Code of Ethics and Conduct, Purpose, Shared Values, Focus Areas, Strategy, Group Policies, and Instructions for the CEO as approved by the Board;

b) Decisions made by the CEO, and Group Instructions and the Delegations of Obligations and Authority as approved by the CEO; and

c) Group Guidelines as approved by the Heads of Group Functions.

There is a set of Instructions and Guidelines connected to this Policy.

Purpose

In Kcell, security measures shall be characterized by appropriate security and risk wareness, prevention, preparedness, and the ability to respond to, and recover from, incidents and changes in the environment. The main drivers for security are:

- Protection of shareholders' value and the Company's assets and investments
- Ensuring that customers' expectations and business agreements are met
- Ensuring that the business strategies and objectives are not jeopardized due to security risks
- Ensuring that laws and regulatory security related requirements are complied with (legal compliance).

PRINCIPLES

The following principles shall apply for the activities under this Policy:
Kcell shall implement security measures, which aims to balance risk exposure, business value, vulnerabilities and threats.

In order to protect business and shareholder value, measures must be taken to protect assets such as personnel, customers, information, IT infrastructure, internal and public networks, as well as office buildings and technical facilities. Information security is vital for ensuring reliable and secure access to information. Kcell shall implement measures to prevent and detect disclosure of sensitive information to unauthorized parties. Special attention shall be given to information affecting user privacy.

Products, services, and key strategic and operational processes must continuously, throughout its life cycle, undergo thorough analysis to identify risks and threats affecting our business. The analysis aims to guide decision making and ensure proper implementation of security measures to meet compliance and balance risk exposure.

Kcell does not accept criminal activities or fraud. Appropriate measures, including data preservation, shall be in place to enable detection and prompt response to security incidents and fraud. All Kcell employees and line managers are obligated to report security incidents and fraud according to established routines.

Kcell must ensure that critical business functions will be available to customers and other stakeholders.

Business continuity plans must be in place for all business critical services to maintain service resilience and recoverability according to business, legal and regulatory demands.

To ensure Kcell's ability to handle unpredictable events, a crisis management organization and corresponding plans must be in place.

Security audits (follow-ups) shall continuously be conducted to ensure implementation of corrective actions and compliance to policies, instructions and legal/regulatory demands.

In case of non-compliance of the Kcell Security Policy any employee, who are aware of any breaches, shall report to the Finance department director .

These principles apply to the extent that they do not place Kcell in violation of laws and regulations of the Republic of Kazakhstan.

ROLES AND RESPONSIBILITIES

Finance department director reporting to the CEO of Kcell is responsible for ensuring that this Policy is duly communicated and implemented, and that the employees within his/her area of responsibility are familiar with and follow this Policy.

All Kcell employees are however individually responsible for reading, understanding and following this Policy. Each employee is also obliged to speak up and raise concerns about actual or possible violations of this Policy. Violations of this Policy can lead to disciplinary action up to and including termination.